대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0004126
Application Number

출 원 년 월 일 : 2003년 01월 21일
Date of Application JAN 21, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 05 월 26 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2003.01.21
【발명의 명칭】	서로 다른 사설망에 위치한 네트워크 장치들 사이의 통신을 지원하는 망접속장치
【발명의 영문명칭】	Gateway for supporting communication between network devices of different private networks
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	정홍식
【대리인코드】	9-1998-000543-3
【포괄위임등록번호】	2003-002208-1
【발명자】	
【성명의 국문표기】	김준형
【성명의 영문표기】	KIM,JUN HYEONG
【주민등록번호】	690628-1052415
【우편번호】	430-015
【주소】	경기도 안양시 만안구 안양5동 현대(아) 101-1610
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 정홍식 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	18 면 18,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	6 항 301,000 원
【합계】	348,000 원
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】

【요약】

서로 다른 사설망에 연결된 네트워크 장치들 사이의 통신을 지원하는 망접속장치가 개시된다. 망접속장치는 사설망에 연결된 호스트로부터 공중망에 연결된 타사설망에 대한 터널 생성 요청메시지가 수신되면, 타사설망의 게이트웨이와 통신하여 VPN터널을 형성한다. 이때, 사설망 및 타사설망의 네트워크 주소가 같거나 어느 한 사설망에 다른 한 사설망의 네트워크 주소가 포함되면, 두 사설망이 VPN터널 내에서 서로 다른 네트워크 주소를 사용하도록 새로운 네트워크 주소 테이블을 생성하고, 사설망에 연결된 호스트 또는 타사설망으로부터 전송된 데이터 패킷에 대해 상기 새로운 네트워크 주소 테이블을 토대로 주소를 변환시켜 포워딩한다. 이에 따라 가정 내 사용자는 이용망을 보다 확장할 수 있어 다양한 커뮤니티 활동을 할 수 있게 되며, 인터넷에서 IPv4 형태의 공인 IP부족 문제를 해결할 수 있게 된다.

【대표도】

도 5

【색인어】

망접속장치, 게이트웨이, 홈네트워크, 사설망, VPN, NAT

【명세서】

【발명의 명칭】

서로 다른 사설망에 위치한 네트워크 장치들 사이의 통신을 지원하는 망접속장치 {Gateway for supporting communication between network devices of different private networks}

【도면의 간단한 설명】

도 1은 본 발명에 따른 망접속장치를 포함하는 네트워크 구성도,

도 2는 도 1에 보인 망접속장치의 개략적인 블록도,

도 3은 확장된 네트워크ID가 서로 다른 두 사설망의 VPN터널 형성과정을 설명하는 신호흐름도,

도 4는 도 3의 과정에 의해 사설망A와 사설망B 사이에 형성된 터널을 통한 호스트A와 호스트B의 패킷전달과정을 설명하는 신호흐름도,

도 5는 확장된 네트워크ID가 서로 일치하는 두 사설망의 VPN터널 형성과정을 설명하는 신호흐름도,

도 6은 도 5의 과정에 의해 사설망A와 사설망B 사이에 형성된 터널을 통한 호스트A와 호스트B의 패킷전달과정을 설명하는 신호흐름도, 그리고

도 7은 사설망A의 확장된 네트워크ID가 사설망B의 확장된 네트워크ID에 포함되는 경우의 두 사설망간 VPN터널 형성과정을 설명하는 신호흐름도이다.

도면의 주요부분에 대한 부호의 설명

100: 게이트웨이 110: 공중망 인터페이스

120: 사설망 인터페이스 130: 메모리부

132, 132': 사설망 연결 관리 테이블

140: 제어부 141: NAT/NAPT처리부

142: IP처리부 143, 143': 사설망DNS처리부

144: DHCP처리부 145, 145': 라우팅부

146, 146': VPN처리부 147: 웹서버/미들웨어서버

148: 암호화처리부 149: 사용자인증처리부

150: ISP(Internet Service Provider)

200: 사설망 210, 310, 320: 호스트

212: 웹브라우저 214: 응용프로그램

300: 인터넷 330: 인터넷DNS서버

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<21> 본 발명은 망접속장치에 관한 것으로서, 특히, 서로 다른 망에 연결된 네트워크 장치들 사이의 통신을 가능하게 하는 망접속장치에 관한 것이다.

<22> 최근 통신기술의 발달과 함께 초고속통신망이 각 가정에 널리 보급되고 있다. 또한, 기업들은 가정 내에서 가전기기를 이용하여 인터넷에 접속할 수 있도록 인터넷 냉장고, 디지털 TV, 셋탑박스 등과 같은 네트워크 기능이 추가된 다양한 디지털 정보가전

기기들을 출시하고 있다. 이처럼 가정 내에서 사용되어지는 가전기기들에 네트워크 기능이 추가되어 정보단말화 됨에 따라 새로운 네트워크 형태인 홈네트워크가 출현하였다.

<23> 홈네트워크를 구성하는 가정내의 전기/전자제품은 유/무선을 통해 인터넷과 연결되므로, 사용자는 가정 및 원격지 등에서 위치에 관계없이 정보를 송수신하는 한편, 전기/전자제품들을 인터넷을 통해 제어할 수 있게 되었다.

<24> 한편, 전기/전자제품을 인터넷과 연결하기 위해서 가정 내에는 새로운 네트워크 장치들과 각 장치에 탑재될 프로그램들이 요구된다. 이러한 장치들 가운데, 인터넷과 홈네트워크를 연결하며, 네트워크 패킷의 흐름을 제어하는 네트워크 장치를 홈게이트웨이(Home Gateway)라 한다.

<25> 현재 가정에서는 ADSL, Cable 모뎀 등의 초보적인 홈게이트웨이를 사용하여 인터넷 서비스제공자(Internet Service Provider: ISP)로부터 하나의 공인 IP(Internet Protocol) 주소를 할당받아 인터넷에 접속할 수 있다.

<26> 그러나 위와 같은 종래 홈게이트웨이는 하나의 홈네트워크 기기에서 인터넷으로의 단순한 연결을 제공할 뿐 다양한 서비스를 제공하지는 못하고 있다. 즉, 가정내 복수의 네트워크 기기 보급, SOHO, 재택근무의 활성화, 가전기기 자동화, 그리고 원격제어 등이 진행됨에 따라 홈게이트웨이에 보다 다양한 서비스가 요구되고 있는 데 반해, 기존의 홈게이트웨이는, 그러한 사용자의 욕구를 만족시키지 못하고 있는 형편이다.

<27> 위와 같은 사용자 요구를 수용하기 위해 홈네트워크에는 사설 IP주소를 이용하는 방안이 제안되었다. 사설 IP주소를 이용하는 방안은, 홈네트워크에 있는 복수

의 네트워크 기기가 하나의 공인 IP주소를 공유하여 인터넷에 접근할 수 있도록 네트워크주소포트변환(Network Address Port Translation: NAPT) 기술이 홈게이트웨이에 적용된다. 또한, 인터넷에 연결되어 있는 원격 사용자가 사설망인 홈네트워크에 접근할 수 있도록 가상사설망(Virtual Private Network: VPN) 기술이 홈게이트웨이에 적용된다.

<28> 그러나 홈게이트웨이가 할당받는 공인 IP주소는 수시로 변하므로 인터넷에 연결되어 있는 사용자가 홈네트워크에 접속하기 위해서는 현재 홈게이트웨이에 할당된 공인 IP주소를 반드시 알고 있어야 한다. 이처럼 ISP로부터 홈게이트웨이에 할당된 가변적인 공인 IP주소를 반드시 알아야 한다는 문제를 해결하기 위하여 홈게이트웨이는 ISP로부터 공인 IP주소를 할당받은 후, 홈게이트웨이의 도메인 이름과 할당받은 공인 IP주소를 인터넷에 위치한 동적 DNS서버에 등록한다.

<29> 또한, 홈게이트웨이는 ISP로부터 하나의 공인 IP주소를 할당받으나, 홈네트워크 환경에서는 복수의 정보기기들이 가정 내에서 사용되므로 하나의 공인 IP주소만으로는 이들을 동시에 인터넷에 연결할 수 없다. 따라서 가정 내에는 사설 IP주소가 사용되어지며 하나의 공인 IP주소를 이용하여 이들을 인터넷에 연결해주는 NAPT 기술이 사용된다.

<30> NAPT는 가정에서 인터넷으로 나가는 패킷이 있는 경우, 홈게이트웨이는 패킷의 출발지 사설 IP주소와 출발전 포트번호를 할당받은 공인 IP주소와 다른 포트번호로 변환하고 이를 NAPT 변환표에 기록한다. 이에 대한 응답 패킷이 인터넷으로부터 홈네트워크로 전송되는 경우 홈게이트웨이는 NAPT 변환표를 참조하여 패킷의 목적지 공인 IP주소와 목적지 포트번호를 사설 IP주소와 포트번호로 변환한 후, 최종목적지로 라우팅한다. 인터넷에서 홈네트워크로 전송된 패킷이 NAPT 변환표에 기록되어 있지 않으면 패킷은 폐기된다.

<31> NAPT기술을 이용하면 홈네트워크에서 인터넷으로 접근은 가능하다. 즉, 사설망 내에 위치한 복수의 네트워크 기기가 하나의 공인 IP주소를 공유하여 인터넷에 접근하는 것이 가능하다. 그러나 인터넷에서 홈네트워크로의 접근은 불가능하며, 이것은 인터넷에 연결되어 있는 외부사용자가 보내는 패킷이 홈게이트웨이를 통과하여 사설망 내부로 변환/라우팅되기 위해서는 NAPT 변환표에 사설 IP주소 및 포트, 홈게이트웨이 포트번호, 공인 IP주소 및 포트, IP프로토콜 등의 정보가 기록되어 있어야 하는 데, 이 정보들을 미리 알 수 없기 때문이다.

<32> 인터넷에 연결되어 있는 외부사용자가 사설망에 있는 네트워크 기기에 접근할 수 있도록 하기 위해 홈게이트웨이에 적용되어지는 기술이 VPN이다. VPN은 적용되는 환경과 네트워크 계층에 따라 여러가지가 있으나, 홈네트워크 환경에서는 일반적으로 PPTP, L2TP 등의 2계층 터널링 프로토콜이 많이 사용된다. 홈게이트웨이에는 VPN서버가 위치하며, 인터넷에 연결되어 있는 원격사용자는 VPN클라이언트로 동작한다. 각 홈네트워크의 홈게이트웨이들은 각각의 홈네트워크에서 VPN서버 또는 VPN클라이언트로 동작할 수 있다. 우선 VPN클라이언트는 인터넷 상에서 공인 IP주소를 이용하여 VPN서버에 터널의 생성을 요청한다. 터널이 형성되면 VPN서버는 VPN클라이언트를 인증한 후, VPN클라이언트에게 홈네트워크의 내부에서 사용할 수 있는 사설 IP주소를 할당한다. VPN클라이언트는 할당받은 사설 IP주소를 이용하여 가상의 네트워크 인터페이스를 만들며, 이것은 홈네트워크에 연결되어 마치 하나의 네트워크인 것처럼 동작한다. VPN클라이언트의 공인 IP주소는 VPN서버까지의 터널을 만드는데 사용되며, 사설 IP주소는 터널을 통하여 연결된 홈네트워크에서 사용된다.

<33> 위와 같이 NAPT와 VPN기술을 홈게이트웨이에 적용하면 가정내 복수의 네트워크 기기를 통해 인터넷에 연결할 할 수 있으며, 인터넷에 위치한 원격 사용자들이 홈네트워크에 연결할 수 있게 된다.

<34> 그러나 위와 같이 NAPT 및 VPN 등의 기술들은 홈네트워크와 인터넷은 서로 연결시켜주고 있지만, 임의의 홈네트워크와 또 다른 홈네트워크 사이의 연결을 제공할 수는 없다는 문제점이 있었다. 즉, 홈네트워크에서는 사설 IP주소가 이용되는 관계로, 서로 다른 공인 IP주소를 사용하는 복수의 홈네트워크가 동일한 사설 IP주소를 사용할 수 있기 때문에 홈네트워크에 연결된 어느 한 호스트에서 데이터를 전송하려는 경우, 자신이 속한 홈네트워크에 있는 호스트와 원격지의 홈네트워크에 속한 호스트의 IP주소가 동일하면, 데이터를 어느 홈네트워크에 속한 호스트에 전송할 지 결정할 수 없어 데이터 전송 에러를 발생시키게 된다.

【발명이 이루고자 하는 기술적 과제】

<35> 본 발명의 목적은 상기와 같은 문제점을 해결하기 위하여 서로 다른 사설망에 연결된 네트워크 장치들 사이의 통신이 가능하도록 서비스를 제공하는 망접속장치를 제공하는 데 있다.

【발명의 구성 및 작용】

<36> 상기의 목적을 달성하기 위한 본 발명의 망접속장치는, 공중망과 연결되는 적어도 하나 이상의 공중망 인터페이스; 사설망과 연결되는 적어도 하나 이상의 사설망 인터페이스; 상기 사설망에 연결된 호스트로부터 상기 공중망에 연결된 타사설망에 대한 터널 생성 요청메시지가 수신되면, 상기 타사설망의 게이트웨이와 통신하여 VPN터널을 형성시

키되, 상기 사설망 및 상기 타사설망의 네트워크 주소가 같거나 어느 한 사설망에 다른 한 사설망의 네트워크 주소가 포함되면, 상기 두 사설망이 VPN터널 내에서 서로 다른 네트워크 주소를 사용하도록 새로운 네트워크 주소 테이블을 생성하고, 상기 사설망에 연결된 호스트 또는 상기 타사설망으로부터 전송된 데이터 패킷에 대해 상기 새로운 네트워크 주소 테이블을 토대로 목적지 주소 또는 출발지 주소를 변환시켜 포워딩하는 제어부;를 포함한다.

<37> 상기 제어부는, 상기 사설망에 연결된 호스트에서 터널 생성을 요청할 수 있도록 터널생성요청페이지를 제공하는 웹서버; 상기 사설망에 연결된 호스트의 상기 타사설망에 대한 터널 생성 요청에 대해 상기 공중망에 연결된 DNS(Domain Name Server)로부터 상기 타사설망 게이트웨이의 공인 IP(Internet Protocol)주소를 획득하는 사설망 DNS처리부; 상기 공중망 인터페이스를 통해 전달된 터널 생성 요청 또는 상기 사설망 인터페이스를 통해 전달된 터널 생성 요청에 따라 서버 또는 클라이언트로 동작하여 요청 대상 사설망과 터널이 형성될 수 있도록 처리하는 VPN(Virtual Private Network)처리부; 및 상기 사설망에서 상기 공중망으로 전송되는 데이터 패킷 또는 상기 공중망에서 상기 사설망으로 전송되는 데이터 패킷에 대해 NAPT프로토콜을 이용하여 사설 IP주소를 공인 IP주소로 변환하거나 공인 IP주소를 사설 IP주소로 변환시키며, 상기 사설망과 상기 타사설망 사이에 상기 VPN 터널이 형성된 경우, NAT 프로토콜을 이용하여 상기 VPN 터널 내에서 주소변환을 수행하는 NAT/NAPT처리부;를 포함한다. 여기서, 상기 웹서버는, 미들웨어서버로 대체 가능하다.

<38> 상기 VPN처리부는, 상기 사설망에 연결된 상기 호스트로부터 상기 타사설망에 대한 상기 터널 생성 요청이 전달되면, 상기 사설망의 네트워크 주소 및 상기 VPN 터널에서

상기 사설망의 네트워크 주소 대신에 사용될 제2 네트워크 주소들을 포함하는 상기 터널 생성 요청 메시지를 상기 타사설망 게이트웨이에 전송한다. 그리고 상기 VPN처리부는 상기 터널 생성 요청에 대해 상기 타사설망의 게이트웨이로부터 상기 타사설망의 네트워크 주소, 상기 제2 네트워크 주소, 및 상기 VPN 터널에서 상기 타사설망의 네트워크 주소 대신에 사용될 제3 네트워크 주소들을 포함하는 응답이 수신되면, 상기 사설망의 네트워크 주소, 상기 타사설망의 네트워크 주소, 상기 제2 네트워크 주소, 상기 제3 네트워크 주소를 포함하는 ACK(Acknowledge)를 상기 타사설망 게이트웨이에 전송한다. 또한, 상기 VPN처리부는, 상기 타사설망에 대한 터널 생성 요청메시지 발생부터 상기 ACK를 전송하기까지의 과정을 통해 사설망간 연결 관리 테이블을 생성한다. 상기 사설망 연결 관리 테이블은, 상기 사설망의 네트워크 주소, 상기 타사설망의 네트워크 주소, 상기 제2 네트워크 주소, 상기 제3 네트워크 주소를 포함하며, 상기 타사설망 게이트웨이의 도메인 이름 및 상기 타사설망 게이트웨이의 VPN 동작에 따른 서버/클라이언트 상태 표시 항목을 더 포함할 수 있다.

<39> 상기 NAT/NAPT처리부는 위와 같이 상기 VPN처리부에서 상기 사설망 연결 관리 테이블을 생성하면, 상기 사설망에 연결된 호스트들에 대하여 NAT(Network Address Table)를 설정한다.

<40> 또한, 상기 DNS처리부는, 상기 타사설망과의 사이에 VPN 터널이 형성된 상태에서 상기 사설망에 연결된 제1 호스트로부터 상기 타사설망에 연결된 제2 호스트에 대한 통신 요구가 전달되면, 상기 제2 호스트의 제3 네트워크 주소를 상기 타사설망의 게이트웨이에 문의하고, 상기 타사설망 게이트웨이로부터 상기 제2 호스트의 제3 네트워크 주소

에 대한 응답이 수신되면, 상기 제1 호스트에 상기 제2 호스트의 제3 네트워크 주소를 전송한다.

<41> 상기 제어부는, 상기 제2 호스트의 제3 네트워크주소를 목적지주소로 하는 데이터 패킷이 상기 제1 호스트로부터 전달되면, 상기 VPN터널을 통해 상기 타사설망 게이트웨이에 포워딩한다.

<42> 한편, 상기 VPN처리부는, 타사설망으로부터 상기 타사설망의 네트워크 주소 및 상기 VPN 터널에서 상기 타사설망의 네트워크 주소 대신에 사용될 제2 네트워크 주소들을 포함하는 터널 요청 메시지가 수신되면, 사설망의 네트워크 주소, 상기 제2 네트워크 주소, 및 상기 VPN 터널에서 상기 사설망의 네트워크 주소 대신에 사용될 제3 네트워크 주소들을 포함하는 응답메시지를 상기 타사설망에 전송한다. 또한, 상기 VPN처리부는, 상기 타사설망으로부터 터널 생성 요청메시지 수신시부터 상기 응답메시지에 대한 ACK를 수신하기까지의 과정을 통해 사설망간 연결 관리 테이블을 생성한다. 상기 사설망 연결 관리 테이블은, 상기 사설망의 네트워크 주소, 상기 타사설망의 네트워크 주소, 상기 제2 네트워크 주소, 상기 제3 네트워크 주소를 포함하며, 상기 타사설망 게이트웨이의 도메인 이름 및 상기 타사설망 게이트웨이의 VPN 동작에 따른 서버/클라이언트 상태 표시 항목을 더 포함할 수 있다.

<43> 상기 NAT/NAPT처리부는, 위와 같이 VPN처리부에서 상기 사설망 연결 관리 테이블을 생성하면, 상기 사설망 연결 관리 테이블을 참조하여 상기 사설망에 연결된 호스트들에 대한 NAT(Network Address Table)를 설정한다.

<44> 또한, 상기 DNS처리부는, 상기 타사설망으로부터 상기 사설망에 연결된 호스트에 대한 문의가 수신되면, 상기 VPN터널 내에서 사용되는 상기 호스트의 네트워크 주소를 응답으로 전송한다.

<45> 상기 제어부는, 상기 타사설망으로부터 상기 호스트의 제3 네트워크 주소를 목적지 주소로 하는 데이터 패킷이 전달되면, 상기 NAT를 참조하여 상기 호스트에 수신된 데이터 패킷을 전송한다.

<46> 이상과 같은 본 발명의 망접속장치는, 사설망에서 공중망(인터넷)으로의 네트워킹 및 인터넷에서 사설망으로의 네트워킹이 가능할 뿐만 아니라 사설망에서 타사설망과의 네트워킹까지도 가능하여 사용자의 네트워킹의 범위를 보다 더 확장시킬 수 있게 된다.

<47> 이하 첨부한 도면을 참조하여 본 발명을 상세하게 설명한다. 이하의 설명에서 복수의 부재에는 복수의 부재를 포괄하는 단일의 부재번호가 이용됨을 명시한다.

<48> 도 1은 본 발명에 따른 홈게이트웨이를 포함하는 네트워크 구성도이다.

네트워크는, 복수의 사설망(200A,200B)과 억세스(Access) 네트워크 및 인터넷(300)을 포함한다. 사설망들(200A,200B)에는 각각 망 내부에 사설망호스트들(210A, 210B,210C,210D)이 연결되며, 인터넷(300)에는 DNS서버(330) 및 복수의 공중망호스트들(310,320)이 연결되어 있다. 그리고 각 사설망(200)과 인터넷(300)은 ISP(150)및 홈게이트웨이(100)를 포함하는 억세스(access) 네트워크를 통해 서로 연결되어 있다.

<49> 사설망(200)과 인터넷(300)을 연결하는 홈게이트웨이(100)는 ISP(150)로부터 공인 IP주소를 할당받고, 할당받은 IP주소에 대해 인터넷에 연결된 DNS서버(330)에 도메인 네임을 등록한다. 또한, 홈게이트웨이(100)는 각 사설망에 위치한 호스트들(210)과

인터넷(300)에 연결된 호스트들(310,320)이 상호 통신할 수 있도록 NAPT프로토콜 및 VPN을 통해 서비스한다. 또한, 홈게이트웨이(100)는 VPN 및 사설 IP주소 할당을 통해 각 사설망(200) 내부에 위치한 호스트들(210A/210C)과 다른 사설망에 연결된 호스트들(210B/210D)이 상호 통신할 수 있도록 서비스한다. 즉, 홈게이트웨이A(100A) 및 홈게이트웨이B(100B)는 각 사설망(예를 들어, 200A)에 위치한 어느 한 호스트(예를 들어, 호스트A)로부터 다른 사설망(200B)에 위치한 호스트(호스트B)와의 연결 요청에 대해, 상대방 홈게이트웨이(100B)와의 통신을 통해 VPN 터널을 생성하고, 각 사설망(200A/200B)에 연결된 호스트들(210)에 대하여 VPN터널에서 사용될 서로 다른 사설 IP주소를 할당한 후, 터널 양단에서 NAT를 통해 사설망A(200A)에 연결된 호스트A(210A) 또는 호스트C(210C)와 사설망B(200B)에 연결된 호스트B(210B) 또는 호스트D(210D)가 상호 통신할 수 있도록 서비스한다.

<50> 도 2는 본 발명의 실시예에 따른 게이트웨이의 블록도이다. 게이트웨이(100)는 공중망 인터페이스(110), 사설망 인터페이스(120), 메모리부(130) 및 제어부(140)를 포함한다.

<51> 인터페이스는 위와 같이 적어도 두개 이상의 네트워크 인터페이스가 구비되며, 적어도 하나는 공중망 인터페이스이고, 적어도 하나는 사설망 인터페이스이다. 공중망 인터페이스(110)는 ADSL, Cable 모뎀, 이더넷(Ethernet) 등에 의해 물리적으로 인터넷(300)에 연결되며, ISP(150)로부터 할당된 하나의 공인 IP주소를 갖는다. 사설망 인터페이스(120)는 이더넷, 무선랜(Wireless LAN), 홈PNA 등 유/무선으로 구성될 수 있으며, 제어부(140)에서 사설 IP주소를 가진다. 사설망에 사용되는 네트워크 주소는

IANA(Internet Assigned Numbers Authority)에 의해 사용이 허가된 주소들 가운데 무작위로 선택된다.

<52> 메모리부(130)는 시스템 운영에 관련된 프로그램 및 새롭게 생성 및 갱신되는 데이터가 저장된다.

<53> 제어부(140)는 NAT(Network Address Table)/NAPT처리부(141), IP(Internet Protocol)처리부(142), DNS(Domain Name Service)처리부(143), DHCP(Dynamic Host Configuration Protocol)처리부(144), 라우팅부(145), VPN처리부(146), 웹/미들웨어 서버(147), 암호화처리부(148), 그리고 사용자인증처리부(149)를 포함한다.

<54> NAT/NAPT처리부(141)는 사설망에서 인터넷으로 전송되는 패킷 또는 인터넷에서 사설망으로 전송되는 패킷에 대해 사설 IP주소를 공인 IP주소로 변환하거나 공인 IP주소를 사설 IP주소로 변환시킨다. 또한, NAT/NAPT처리부(141)는 VPN 터널을 이용하여 사설망끼리 연결된 경우, NAT 프로토콜을 이용하여 VPN 터널 내에서 주소변환을 수행한다. NAT/NAPT처리부(141)는 메모리부(130)에 NAT 및 NAPT 테이블을 생성 및 지속적으로 갱신한다.

<55> IP처리부(142)는 공중망 인터페이스(110) 및 사설망 인터페이스(120)에서 전달된 패킷의 IP 데이터그램(datagram)에 대한 처리를 수행한다.

<56> 라우팅부(145)는 공중망에 연결된 외부 호스트 및 타사설망에 연결된 호스트와의 최적경로를 설정한다. 라우팅부(145)는 메모리부(130)에 라우팅테이블을 생성 및 지속적으로 갱신한다.

<57> DNS처리부(146)는 사설망 내부의 호스트들에 대한 도메인 이름 및 사설 IP주소를 관리한다. 또한, DNS처리부(146)는 사설망 내부의 호스트로부터 사설망 외부의 호스트에 대한 문의가 발생하면 인터넷에 위치한 DNS서버(330) 또는 타사설망 전단에 위치한 홈게이트웨이로부터 답변을 구하여 응답한다. DNS처리부(146)는 사설망 내부의 호스트들과 관련한 DNS테이블을 관리한다.

<58> DHCP처리부(144)는 사설망 내부의 네트워크 장치가 부팅될 때, 사설망 내부의 호스트들로부터 사용할 수 있는 사설 IP주소, 게이트웨이 주소, DNS처리부 주소 등의 요청에 대해 응답한다. DHCP처리부(144)는 응답의 일부로 호스트의 도메인 이름을 획득하며, 획득한 도메인 이름을 DNS처리부(146)에 전달하여 DNS테이블이 생성 및 갱신될 수 있도록 한다.

<59> 웹(WEB)/미들웨어(Middleware)서버(147)는 사설망의 사용자가 다른 사설망과의 사이에 터널 생성을 요청할 수 있는 수단을 제공한다. 사용자는 웹브라우저 또는 미들웨어 클라이언트를 이용하여 서비스를 요청할 수 있다.

<60> VPN처리부(146)는 인터넷에 위치한 호스트에 대하여 VPN서버로 동작하며, 다른 사설망과의 연결이 가능하도록 VPN서버 또는 VPN클라이언트로 동작한다. 또한, VPN처리부(146)는 사설망 내부에 위치한 호스트로부터 WEB/Middleware서버(147)를 통해 다른 사설망과의 연결이 요청되면, 타사설망과 통신하여 VPN터널을 형성하고, 사설망의 네트워크 주소에 따라 VPN터널의 끝에 NAT를 설정한다. 다른 사설망과의 연결에 필요한 정보들은 사설망 연결 관리 테이블을 생성하여 관리하며, 테이블로 생성된 데이터들은 메모리부(130)에 저장된다. 사설망 연결 관리 테이블은 자체 사설망의 네트워크 주소, 타사설망의 네트워크 주소, VPN터널 내에서 사용될 자체 사설망의 네트워크 주소, VPN터널 내에

서 사용될 타사설망의 네트워크 주소를 포함하며, 상대 사설망 게이트웨이의 도메인 이름 및 상대 사설망 게이트웨이의 VPN 동작에 따른 서버/클라이언트 상태 표시 항목을 더 포함할 수 있다.

<61> 암호화처리부(148)는 사설망과 공중망 사이 또는 사설망과 타사설망 사이에 전달되는 패킷에 대해 암호화를 수행한다.

<62> 사용자인증처리부(149)는 공중망으로부터 사설망에 접근하기 원하는 외부 사용자 및 사설망에서 게이트웨이에 대한 설정변경 등을 위해 접근하는 사용자에 대해 인증절차를 수행한다.

<63> 위와 같은 게이트웨이는 타사설망과 VPN터널을 형성할 때, 다음과 같은 3가지 경우에 따라 대응되는 동작을 수행한다. 각 경우에 대해서 도 1을 참조하여 설명한다.

<64> 첫째, 사설망A(200A)와 사설망B(200B)의 확장된 네트워크 ID(네트워크 ID와 서브넷 마스크의 곱)가 서로 다른 경우(case1)이다. 예를 들어, 사설망A(200A)의 네트워크 ID가 10.0.0.0/24, 사설망B(200B)의 네트워크 ID는 10.0.1.0/24로 설정되었을 때(case1), 사설망A(200A)의 확장된 네트워크 ID는 10.0.0.x가 되고, 사설망B의 확장된 네트워크 주소는 10.0.1.x.가 되어 서로 다르다. 이 경우, 사설망A와 사설망B는 VPN터널을 형성하는 것만으로 상호 통신이 가능하게 된다.

<65> 둘째, 사설망A(200A)와 사설망B(200B)의 확장된 네트워크 ID가 서로 일치하는 경우(case2)이다. 예를 들어, 사설망A와 사설망B의 네트워크 ID가 모두 10.0.0.0/24로 설정되었을 때(case2), 사설망A(200A) 및 사설망B(200B) 모두 확장된 네트워크 ID는 10.0.0.x가 되어 서로 일치한다. 이 경우, 사설망A(200A)에 위치한 호스트A(210A)가 사

설망B(200B)에 위치한 호스트B(210B)에게 패킷을 보내려 할 때, 호스트C(210C)가 호스트B(120B)와 같은 IP주소를 가졌다면, 홈게이트웨이A(100A)는 호스트A(210A)로부터 전송된 패킷을 호스트B(210B)에게 전송해야 하는지 또는 호스트C(210C)에 전송해야 하는지를 알 수 없어 전송에러를 발생시키며, 두 사설망 사이에 통신이 이루어지지 않게 된다. 따라서, 이 경우에는, 사설망A(200A)와 사설망B(200B) 사이에 형성된 터널에서 사용될 수 있는 새로운 IP주소를 할당한다. 예를 들어, 사설망A에는 10.0.1.0/24, 사설망B에는 10.0.2.0/24의 네트워크 주소를 할당한 후, VPN터널의 양단에서 NAT가 수행되도록 한다. 결과적으로, 사설망A(200A)에서 사설망B(200B)에 위치한 호스트(210B/210D)를 바라보면, 사설망B(200B)에 위치한 호스트는 10.0.2.x의 네트워크 주소를 가진 것으로 인식되며, 사설망B(200B)에서는 사설망A(200A)에 위치한 호스트(210A/210C)에 대해 10.0.2.y의 네트워크 주소를 가진 것으로 인식하게 되므로, 사설망A(200A)의 호스트(210A/210C)와 사설망B(200B)의 호스트(210B/210D)는 상호 통신이 가능하게 된다.

<66> 셋째, 사설망A의 네트워크ID가 사설망B의 네트워크ID에 포함되는 경우(case3)이다. 예를 들어, 사설망A(200A)는 10.0.0.0/24, 사설망B(200B)는 10.0.0.0/16과 같이 주어졌을 때(case3), 사설망A(200A)의 확장된 네트워크ID는 10.0.0.x, 사설망B(200B)의 확장된 네트워크ID는 10.0.x.x로 서로 다르지만, 10.0.0.x는 10.0.x.x의 일부로 포함된다. 이 경우에도 사설망A(200A)와 사설망B(200B) 사이에 VPN터널을 만들고 사설망A(200A)에는 10.0.1.0/24, 사설망B(200B)에는 10.1.0.0/16의 네트워크 주소를 할당한 후 터널의 양끝에서 NAT를 수행한다. 결과적으로 사설망A(200A)에서 사설망B(200B)에 위치한 호스트를 바라보면 10.1.x.y의 주소를 가진 것으로 보이며, 사설망B(200B)에서 사설망A(200A)에

위치한 호스트를 바라보면 10.0.1.z의 주소를 가진 것으로 보이므로 사설망A(200A)의 호스트와 사설망B(200B)의 호스트는 서로 통신할 수 있게 된다.

<67> 위의 3가지 경우에서 사설망A(200A)와 사설망B(200B)의 확장된 네트워크ID가 서로 다르면 그 사이에 VPN 터널을 만드는 것만으로도 별다른 설정 없이 서로 통신을 할 수 있으므로, 홈게이트웨이의 내부의 사설망 네트워크 주소는 가급적 서로 다르도록 무작위로 설정하는 것이 바람직함을 알 수 있다.

<68> 이하, 위 세가지 경우에 따른 두 사설망 사이의 VPN터널 형성 및 패킷전달과정을 설명한다.

<69> 도 3은, 확장된 네트워크ID가 서로 다른 두 사설망의 VPN터널 형성과정을 설명하는 신호흐름도이다. 먼저, 게이트웨이A(100A)의 웹서버(147)에서 제공되는 터널형성요청페이지를 사설망A(200A)의 사용자가 호스트A(210A)에서 웹브라우저 (212)를 통해 사설망B(200B)와의 터널 생성을 요청하면, 사설망A(200A)와 사설망B(200B) 사이의 터널 생성 요청을 받은 게이트웨이A(100A)는 DNS처리부(143)를 통해 인터넷에 위치한 DNS 서버(330)로부터 게이트웨이B(100B)의 공인IP주소(211.32.119.136)를 얻는다. 다음으로 게이트웨이A(100A)는 VPN처리부(146)에서 클라이언트 프로그램을 구동하여 게이트웨이B(100B)의 VPN처리부(146')에 터널 생성을 요청한다. 사설망간의 터널 생성 요청 메시지에는 사설망A(200A)의 네트워크 주소(10.0.0.0/24), VPN 터널 내에서 사설망A(200A)의 네트워크 주소 대신에 사용되어질 네트워크 주소들(10.0.0.0/24, 10.0.1.0/24, 10.0.2.0/24, ...)이 포함된다. 이때, 사설망A(200A)와 사설망B(200B)의 네트워크 주소가 서로 다르면, VPN터널 내에서 NAT가 필요 없으므로 사설망A의 주소 (10.0.0.0/24)가

그대로 선택되어지며, 사설망A와 사설망B의 확장된 네트워크 주소가 일치하는 경우에는 10.0.1.0/24, 10.0.2.0/24, ... 중에서 사용 가능한 것이 선택된다.

<70> 게이트웨이B(100B)는 게이트웨이A(100A)에서 사설망간 터널 생성 요청 메시지가 전송되면, VPN처리부(146)에서 사설망간의 터널 생성 응답메시지를 게이트웨이A(100A)에 전송한다. 응답메시지에는 사설망B(200B)의 네트워크 주소(10.0.1.0/24), VPN 터널 내에서 사설망A(200A)의 네트워크 주소 대신에 사용되어질 네트워크 주소(10.0.0.0/24), VPN 터널 내에서 사설망B(200B)의 네트워크 주소 대신에 사용되어질 네트워크 주소들(10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24, ...)이 포함된다.

<71> 응답메시지를 수신한 게이트웨이A(100A)는 사설망간의 터널 생성 ACK를 게이트웨이B(100B)에게 전송한다. ACK는 사설망A(200A)의 네트워크 주소(10.0.0.0/24), 사설망B(200B)의 네트워크 주소(10.0.1.0/24), VPN 터널 내에서 사설망A(200A)의 네트워크 주소 대신에 사용할 네트워크 주소(10.0.0.0/24), VPN 터널 내에서 사설망B(200B)의 네트워크 주소 대신에 사용할 네트워크 주소(10.0.1.0/24)를 포함한다. 이때, 사설망A(200A)의 주소와 VPN 터널 내에서 사설망A(200A)의 네트워크 주소 대신에 사용할 네트워크 주소가 일치하면, VPN 터널 내에서 NAT가 일어나지 않음을 의미하며, 일치하지 않으면 NAT가 일어남을 의미한다.

<72> ACK 메시지를 주고받은 후, 게이트웨이A(100A)와 게이트웨이B(100B)에는 각각 사설망 연결 관리 테이블(132,132')이 생성된다. 사설망 연결 관리 테이블(132)은 상대편 게이트웨이의 도메인 이름, 상대편 게이트웨이가 VPN 서버인지 클라이언트인지를 표시하는 항목, 사설망A(200A)의 네트워크 주소, 사설망B(200B)의 네트워크 주소, VPN 터널 내에

서 사설망A(200A)의 네트워크 주소 대신에 사용할 네트워크 주소, VPN 터널 내에서 사설망B(200B)의 네트워크 주소 대신에 사용할 네트워크 주소 등이 포함된다.

<73> 게이트웨이A(100A)가 생성하는 테이블을 살펴보면, 게이트웨이B(100B)의 도메인 이름(게이트웨이B), 게이트웨이B는 VPN 서버임을 표시하는 항목(서버), 사설망A의 네트워크 주소(10.0.0.0/24), 사설망B의 네트워크 주소(10.0.1.0/24), VPN 터널 내에서 사설망A의 네트워크 주소 대신에 사용할 네트워크 주소(10.0.0.0/24), VPN 터널 내에서 사설망B의 네트워크 주소 대신에 사용할 네트워크 주소(10.0.1.0/24) 등을 포함한다.

<74> 위와 같이 두 사설망 사이에 ACK신호가 교환되면, 게이트웨이A(100A)와 게이트웨이B(100B) 사이에 VPN터널이 형성되며, 터널 내에 PPP 연결이 생성된다. 이후, 호스트A(210A)로부터 게이트웨이A(100A)의 VPN터널 끝으로 전달되어진 패킷은 PPP 연결을 통하여 게이트웨이B(100B)의 VPN터널 끝으로 전달된다.

<75> 도 4는 도 3의 과정에 의해 사설망A(200A)와 사설망B(200B) 사이에 형성된 터널을 통한 호스트A(210A)와 호스트B(210B) 사이의 패킷 전달과정을 설명하는 신호흐름도이다. 먼저, 사설망A(200A)의 사용자가 호스트B(210A)의 도메인 이름을 알고 있으며, 호스트A(210A)에 설치된 응용프로그램은 호스트B(210B)의 도메인 이름에 대응하는 IP주소를 알기 위하여 게이트웨이A(100A)에게 DNS문의를 전송한다. 그러면 게이트웨이A(100A)의 DNS처리부(143)는 먼저 사설망 연결 관리 테이블(132)을 조사한다. 그리고 사설망A(200A)와 사설망B(200B) 사이에 VPN터널이 설정되어 있으면, 게이트웨이B(100B)에게 호스트B(210B)에 대한 DNS 문의를 보낸다.

<76> 위와 같이 게이트웨이A(100A)에서 게이트웨이B(100B)에 DNS 문의가 전송되면, 게이트웨이B(100B)의 DNS처리부(143')는 호스트B(210B)의 네트워크 주소 대신에 VPN터널 내

에서 호스트B(210B)를 표시하는 네트워크 주소(10.0.1.5)를 내용으로 응답메시지를 게이트웨이A(100A)에 전송한다.

<77> 게이트웨이A(100A)는 게이트웨이B(100B)의 DNS처리부(143')로부터 호스트B(210B)에 대해 응답된 사설IP주소(10.0.1.5)를 호스트A(210A)에게 포워딩한다.

<78> 호스트A(210A)는 게이트웨이A(100A)로부터 호스트B(210B)의 사설IP주소가 수신되면, 목적지 주소에는 수신된 사설IP주소(10.0.1.5)를, 출발지 주소에는 호스트A(210A)의 사설IP 주소(10.0.04)를 기입하여 패킷을 게이트웨이A(100A)에 전송한다.

<79> 게이트웨이A(100A)는 호스트A(210A)로부터 패킷이 수신되면, 수신한 패킷을 라우팅 테이블(145)과 포워딩 설정을 참조하여 게이트웨이A(100A)의 터널 끝으로 패킷을 전달한다. 게이트웨이A(100A)와 게이트웨이B(100B) 사이의 VPN터널 내에는 PPP 연결이 설정되어 있으므로 게이트웨이A(100A)의 터널 끝으로 보내진 패킷은 게이트웨이B(100B)의 터널 끝으로 전달된다.

<80> 게이트웨이B(100B)는 VPN터널을 통해 패킷이 전달되면, 라우팅 테이블(145')과 포워딩 설정을 참조하여 호스트B(210B)에게 패킷을 포워딩한다.

<81> 호스트B(210B)는 패킷이 수신되면, 출발지 주소에 호스트B(210B)의 사설IP 주소(10.0.1.5)를, 목적지 주소에 호스트A(210A)의 사설IP 주소(10.0.04)를 기입하여 응답을 보낸다.

<82> 이후, 호스트A(210A)와 호스트B(210B)는 사설망A(200A) 및 사설망B(200B) 사이에 형성된 터널을 통해 위 패킷 전달과정을 반복하게 된다.

<83> 도 5는 확장된 네트워크ID가 서로 일치하는 두 사설망의 VPN터널 형성과정을 설명하는 신호흐름도이다. 먼저, 게이트웨이A(100A)의 웹서버(147)에서 제공되는 터널형성 요청페이지를 사설망A(200A)의 사용자가 호스트A(210A)에서 웹브라우저(212)를 통해 사설망B(200B)와의 터널 생성을 요청하면, 사설망A(200A)와 사설망B(200B) 사이의 터널 생성 요청을 받은 게이트웨이A(100A)는 DNS처리부(143)를 통해 인터넷에 위치한 DNS서버(330)로부터 게이트웨이B(100B)의 공인IP주소(211.32.119.136)를 얻는다. 다음으로 게이트웨이B(100B)의 공인IP주소를 얻은 게이트웨이A(100A)는 VPN처리부(146)에서 클라이언트 프로그램을 구동하여 게이트웨이B(100B)의 VPN처리부(146')에 사설망간 터널 생성을 요청한다. 사설망간의 터널 생성 요청메시지에는 사설망A(200A)의 네트워크 주소(10.0.0.0/24), VPN 터널 내에서 사설망A(200A)의 네트워크 주소 대신에 사용되어질 네트워크 주소들(10.0.0.0/24, 10.0.1.0/24, 10.0.2.0/24, ...)이 포함된다.

<84> 게이트웨이B(100B)의 VPN처리부(146')는 게이트웨이A(100A)로부터 터널 생성 요청이 수신되면, 사설망간의 터널 생성 요청에 대한 응답메시지를 게이트웨이A(100A)에 전송한다. 응답메시지에는 사설망B(200B)의 네트워크 주소(10.0.0.0/24), VPN 터널 내에서 사설망A(200A)의 네트워크 주소 대신에 사용되어질 네트워크 주소(10.0.1.0/24), VPN 터널 내에서 사설망B(200B)의 네트워크 주소 대신에 사용되어질 네트워크 주소들(10.0.2.0/24, 10.0.3.0/24, 10.0.4.0/24, ...)이 포함된다.

<85> 게이트웨이A(100A)는 게이트웨이B(100B)로부터 응답메시지를 수신하면, 사설망간의 터널 생성 ACK를 게이트웨이B(100B)에게 보낸다. ACK는 사설망A(200A)의 네트워크 주소(10.0.0.0/24), 사설망B(200B)의 네트워크 주소(10.0.0.0/24), VPN 터널 내에서 사설망A(100A)의 네트워크 주소 대신에 사용할 네트워크 주소(10.0.1.0/24), VPN터널 내에서

사설망B(200B)의 네트워크 주소 대신에 사용할 네트워크 주소(10.0.2.0/24)를 포함한다. 사설망A(200A)의 주소와 VPN터널 내에서 사설망A(200A)의 네트워크 주소 대신에 사용할 네트워크 주소가 일치하지 않으므로, 게이트웨이A(100A)는 NAT프로토콜에 의해 주소변환이 사용될 것으로 인식한다.

<86> ACK 메시지를 주고받은 후, 게이트웨이A(100A)와 게이트웨이B(100B)에는 각각 사설망 연결 관리 테이블(132,132')이 생성된다. 사설망 연결 관리 테이블(132)은 상대편 게이트웨이(100)의 도메인 이름, 상대편 게이트웨이(100)가 VPN 서버인지 클라이언트인지를 표시하는 항목, 사설망A(200A)의 네트워크 주소, 사설망B(200B)의 네트워크 주소, VPN 터널 내에서 사설망A(200A)의 네트워크 주소 대신에 사용할 네트워크 주소, VPN 터널 내에서 사설망B(200B)의 네트워크 주소 대신에 사용할 네트워크 주소 등을 포함한다.

<87> 게이트웨이A(100A)가 생성하는 테이블을 살펴보면, 게이트웨이B(100B)의 도메인 이름(게이트웨이B), 게이트웨이B는 VPN 서버임을 표시하는 항목(서버), 사설망A(200A)의 네트워크 주소(10.0.0.0/24), 사설망B(200B)의 네트워크 주소(10.0.0.0/24), VPN터널 내에서 사설망A(200A)의 네트워크 주소 대신에 사용할 네트워크 주소(10.0.1.0/24), VPN터널 내에서 사설망B(200B)의 네트워크 주소 대신에 사용할 네트워크 주소(10.0.2.0/24) 등을 포함한다.

<88> 위와 같은 과정을 통해 게이트웨이A(100A)와 게이트웨이B(100B) 사이는 VPN터널이 형성되며, 터널 내에 PPP 연결이 생성된다. 이후, 게이트웨이A(100A)의 VPN 터널 끝으로 전달되어진 패킷은 PPP 연결을 통하여 게이트웨이B(100B)의 VPN 터널 끝으로 전달된다.

<89> VPN 터널이 생성되고, PPP 연결이 끝나면 게이트웨이A(100A)는 사설망 연결 관리 테이블(132)을 참조하여 VPN 터널의 게이트웨이A(100A)에 NAT를 설정한다. NAT를 설정하면, 패킷이 사설망A(200A)에서 게이트웨이A(100A)를 지나 VPN터널로 보내질 때, 출발지 주소 10.0.0.x는 10.0.1.x로 변환되며, 패킷이 VPN터널로부터 게이트웨이A(100A)를 지나 사설망A로 보내질 때 목적지 주소 10.0.1.y가 10.0.0.y로 변환된다. 또한 게이트웨이B도 VPN 터널의 게이트웨이B 쪽에 NAT를 설정한다.

<90> 도 6은 도 5의 과정에 의해 사설망A와 사설망B 사이에 형성된 터널을 통한 호스트A(210A)와 호스트B(210B) 사이의 패킷 전달과정을 설명하는 신호흐름도이다. 먼저 사설망A(200A)의 사용자가 호스트B(210B)의 도메인 이름을 알고 있으며, 호스트A(210A)에 설치된 응용프로그램(214)이 게이트웨이A(100A)에게 호스트B(210B)에 대한 DNS를 문의하면, 게이트웨이A(100A)의 DNS처리부(143)는 사설망 연결 관리 테이블(132)을 조사한다. 그리고 사설망A(200A)와 사설망B(200B) 사이에 VPN터널이 설정되어 있으면, 터널을 통과하는 패킷에 대한 NAT가 필요한 것으로 인식되어 있으므로, 게이트웨이B(100B)에게 호스트B(210B)의 VPN터널에서 사용될 사설IP주소를 알기 위하여 DNS문의를 게이트웨이B에게 전송한다.

<91> 게이트웨이B(100B)의 DNS처리부(143')는 호스트B(210B)에 대한 문의가 수신되면, 호스트B(210B)의 VPN터널 내에서 사용되는 IP주소(10.0.2.5)를 게이트웨이A(100A)에 응답메시지를 전송하며, 게이트웨이A(100A)는 이를 호스트A(210A)에게 재전송한다.

<92> 이후, 호스트A(210A)는 호스트B(210B)로 패킷을 보내기 위하여 패킷을 게이트웨이A((100A)에 전송한다. 패킷의 목적지 주소는 10.0.2.5가 기입되며, 출발지 주소는 10.0.0.4가 기입된다.

<93> 게이트웨이A(100A)는 호스트A(210A)로부터 호스트B(210B)를 목적지로 하는 패킷이 수신되면, 라우팅 테이블과 포워딩 설정을 참조하여 게이트웨이A(100A)의 터널 끝으로 패킷을 전달한다. 그러면 게이트웨이A(100A)의 VPN터널 끝에는 NAT가 설정되어 있으므로, 출발지 주소 10.0.0.4는 10.0.1.4로 변환된다. 그리고 게이트웨이A(100A)와 게이트웨이B((100B) 사이의 터널에는 PPP 연결이 설정되어 있으므로, NAT를 통해 출발지 주소가 변환된 패킷은 게이트웨이B(100B)의 터널 끝으로 전송된다.

<94> 게이트웨이B(100B)는 위와 같이 출발지 주소가 NAT를 통해 변경되어 게이트웨이B(100B)의 터널 끝으로 전달된 패킷에 대해 게이트웨이B(100B)의 VPN 터널 끝에 설정된 NAT를 통해 목적지 주소 10.0.2.5를 10.0.0.5로 변환시킨다. 이렇게 NAT를 통해 목적지 주소가 변환된 패킷은 라우팅 테이블과 포워딩 설정을 참조하여 호스트B(210B)에게 전달된다.

<95> 이후, 호스트B(210B)는 호스트A(210A)로 응답을 보내며, 위 패킷 전달과정의 반복에 의해 통신이 이루어진다.

<96> 도 7은 사설망A의 확장된 네트워크ID가 사설망B의 확장된 네트워크ID에 포함되는 경우의 두 사설망간 VPN터널 형성과정을 설명하는 신호흐름도이다. 먼저, 게이트웨이A(100A)의 웹서버(147)에서 제공되는 터널형성요청페이지를 사설망A(200A)의 사용자가 호스트A(210A)에서 웹브라우저(212)를 통해 불러온 후, 사설망B(200B) 에 대해 터널 생성을 요청하면, 사설망A(200A)와 사설망B(200B) 사이의 터널 생성 요청을 받은 게이트웨이A(100A)는 DNS처리부(143)를 통해 인터넷에 위치한 DNS서버(330)로부터 게이트웨이B(100B)의 공인IP주소(211.32.119.136)를 얻는다. 다음으로 게이트웨이B(100B)의 공인IP주소를 얻은 게이트웨이A(100A)는 VPN처리부(146)에서 클라이언트 프로그램을 구동하여

게이트웨이B(100B)의 VPN처리부에 사설망간 터널 생성을 요청한다. 사설망간의 터널 생성을 요청하는 메시지에는 사설망A의 네트워크 주소(10.0.0.0/24), VPN터널 내에서 사설망A의 네트워크 주소 대신에 사용될 네트워크 주소들(10.0.0.0/24, 10.0.1.0/24, 10.0.2.0/24, ...)이 포함된다.

<97> 게이트웨이B(100B)는 게이트웨이A(100A)로부터 터널 형성 요청메시지가 수신되면, VPN처리부(146')에서 사설망간의 터널 생성 응답메시지를 보낸다. 응답메시지는 사설망B의 네트워크 주소(10.0.0.0/16), VPN 터널 내에서 사설망A의 네트워크 주소 대신에 사용될 네트워크 주소(10.0.1.0/24), VPN 터널 내에서 사설망B의 네트워크 주소 대신에 사용될 네트워크 주소들(10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16, ...)을 포함한다.

<98> 게이트웨이A(100A)는 게이트웨이B(100B)로부터 응답메시지가 수신되면, 사설망간의 터널 생성 ACK를 게이트웨이B(100B)에 전송한다. ACK는 사설망A의 네트워크 주소(10.0.0.0/24), 사설망B의 네트워크 주소(10.0.0.0/16), VPN터널 내에서 사설망A의 네트워크 주소 대신에 사용할 네트워크 주소(10.0.1.0/24), VPN 터널 내에서 사설망B의 네트워크 주소 대신에 사용할 네트워크 주소(10.1.0.0/24)를 포함한다. 사설망A의 주소와 VPN 터널 내에서 사설망A의 네트워크 주소 대신에 사용할 네트워크 주소가 일치하지 않으므로, 게이트웨이A(100A)는 NAT가 사용되어야 할 것으로 인식한다.

<99> ACK 메시지를 주고받은 후, 게이트웨이A(100A)와 게이트웨이B(100B)에는 사설망 연결 관리 테이블(132,132')이 생성된다. 게이트웨이A(100A)가 생성하는 테이블(132)을 살펴보면, 게이트웨이B(100B)의 도메인 이름, 게이트웨이B(100B)는 VPN 서버임을 표시하는 항목, 사설망A의 네트워크 주소(10.0.0.0/24), 사설망B의 네트워크 주소(10.0.0.0/16), VPN 터널 내에서 사설망A의 네트워크 주소 대신에 사용할 네트워크 주소(10.0.1.0/24),

VPN 터널 내에서 사설망B의 네트워크 주소 대신에 사용할 네트워크 주소(10.1.0.0/16) 등을 포함한다.

<100> 위와 같은 과정을 통해 게이트웨이A(100A)와 게이트웨이B(100B) 사이의 VPN 터널 내에 PPP 연결이 생성된다. 이후, 게이트웨이A(100A)의 VPN 터널 끝으로 전달되어진 패킷은 PPP 연결을 통하여 게이트웨이B(100B)의 VPN 터널 끝으로 전달된다.

<101> 다음으로, VPN 터널이 생성되고 PPP 연결이 끝나면 게이트웨이A(100A)는 사설망 연결 관리 테이블(132)을 참조하여 VPN 터널의 게이트웨이A(100A) 쪽에 NAT를 설정한다. NAT를 설정하면 패킷이 사설망A에서 게이트웨이A(100A)를 지나 VPN 터널로 보내질 때, 출발지 주소 10.0.0.x는 10.0.1.x로 변환되며, 패킷이 VPN 터널로부터 게이트웨이A(100A)를 지나 사설망A로 보내질 때 목적지 주소 10.0.1.y가 10.0.0.y로 변환된다. 마찬가지로, 게이트웨이B(100B)도 VPN 터널의 게이트웨이B(100B) 쪽에 NAT를 설정한다.

<102> 위와 같이 게이트웨이A(100A) 및 게이트웨이B(100B) 사이에 형성된 VPN터널 양단에 NAT가 설정되면, 이후, 호스트A(210A)와 호스트B(210B)는 도 6에 보인 데이터 패킷 전달과정을 통해 상호 통신을 할 수 있게 된다.

【발명의 효과】

<103> 본 발명의 망접속장치는 사설망과 공중망 또는 사설망과 사설망간 연결이 가능하여 사용자의 이용망을 보다 확장시킬 수 있어 가정 내 사용자의 편의를 도모할 수 있으며, 최근 새롭게 부상되는 홈네트워크에서 타 홈네트워크 사용자와 보다 다양하게 커뮤니티를 활성화 할 수 있을 뿐만 아니라 홈네트워크 사이에서 장치 또는 자료를 공유하는 서비스가 가능해지므로 홈네트워크 시장의 활성화에 기여할 수 있다.

<104> 또한, 현재의 IPv4환경에서 공인IP주소의 부족현상을 해소할 수 있어 전체 네트워크의 성능을 향상시킬 수 있게 된다.

<105> 이상에서는 본 발명의 바람직한 실시예에 대해서 도시하고 설명하였으나, 본 발명은 상술한 특정의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능한 것은 물론이고, 그와 같은 변경은 청구범위 기재의 범위 내에 있게 된다.

【특허청구범위】

【청구항 1】

공중망과 연결되는 적어도 하나 이상의 공중망 인터페이스;

사설망과 연결되는 적어도 하나 이상의 사설망 인터페이스; 및

상기 사설망에 연결된 호스트로부터 상기 공중망에 연결된 타사설망에 대한 터널 생성 요청메시지가 수신되면, 상기 타사설망의 게이트웨이와 통신하여 VPN터널을 형성시키되, 상기 사설망 및 상기 타사설망의 네트워크 주소가 같거나 어느 한 사설망에 다른 한 사설망의 네트워크 주소가 포함되면, 상기 두 사설망이 VPN터널 내에서 서로 다른 네트워크 주소를 사용하도록 새로운 네트워크 주소 테이블을 생성하고, 상기 사설망에 연결된 호스트 또는 상기 타사설망으로부터 전송된 데이터 패킷에 대해 상기 새로운 네트워크 주소 테이블을 토대로 주소를 변환시켜 포워딩하는 제어부;를 포함하는 것을 특징으로 하는 망접속장치.

【청구항 2】

제 1항에 있어서,

상기 제어부는,

상기 사설망에 연결된 호스트에서 터널 생성을 요청할 수 있도록 터널생성요청페이지를 제공하는 웹서버;

상기 사설망에 연결된 호스트의 상기 타 사설망에 대한 터널 생성 요청에 대해 상기 공중망에 연결된 DNS(Domain Name Server)로부터 상기 타사설망 게이트웨이의 공인 IP(Internet Protocol)주소를 획득하는 사설망 DNS처리부;

상기 공중망 인터페이스를 통해 전달된 터널 생성 요청 또는 상기 사설망 인터페이스를 통해 전달된 터널 생성 요청에 따라 서버 또는 클라이언트로 동작하여 요청 대상 사설망과 터널이 형성될 수 있도록 처리하는 VPN(Virtual Private Network)처리부; 및

상기 사설망에서 공중망으로 전송되는 데이터 패킷 또는 상기 공중망에서 사설망으로 전송되는 데이터 패킷에 대해 NAPT(Network Address Port Table)프로토콜을 이용하여 사설 IP주소를 공인 IP주소로 변환하거나 공인 IP주소를 사설 IP주소로 변환시키며, 상기 사설망과 상기 타사설망 사이에 상기 VPN 터널이 형성된 경우, NAT(Network Address Table)프로토콜을 이용하여 상기 VPN 터널 내에서 사설IP주소의 주소변환을 수행하는 NAT/NAPT처리부;를 포함하는 것을 특징으로 하는 망접속장치.

【청구항 3】

제 2항에 있어서,

상기 VPN처리부는, 상기 사설망에 연결된 상기 호스트로부터 상기 타사설망에 대한 상기 터널 생성 요청이 전달되면, 상기 터널 생성 요청 메시지를 상기 타사설망 게이트웨이에 전송하며, 상기 타사설망의 게이트웨이로부터 상기 터널 생성 요청에 대한 응답이 수신되면, ACK(Acknowledge)를 상기 타사설망 게이트웨이에 전송하는 것을 특징으로 하는 망접속장치.

【청구항 4】

제 3항에 있어서,

상기 타사설망에 대한 터널 생성 요청 메시지는, 상기 사설망의 네트워크 주소 및 상기 VPN 터널에서 상기 사설망의 네트워크 주소 대신에 사용될 제2 네트워크 주소들을 포함하는 것을 특징으로 하는 망접속장치.

【청구항 5】

제 3항에 있어서,

상기 VPN처리부는, 타사설망으로부터 상기 타사설망의 네트워크 주소 및 상기 VPN 터널에서 상기 타사설망의 네트워크 주소 대신에 사용될 제2 네트워크 주소들을 포함하는 터널 요청 메시지가 수신되면, 사설망의 네트워크 주소, 상기 제2 네트워크 주소, 및 상기 VPN 터널에서 상기 사설망의 네트워크 주소 대신에 사용될 제3 네트워크 주소들을 포함하는 응답메시지를 상기 타사설망에 전송하는 것을 특징으로 하는 망접속장치.

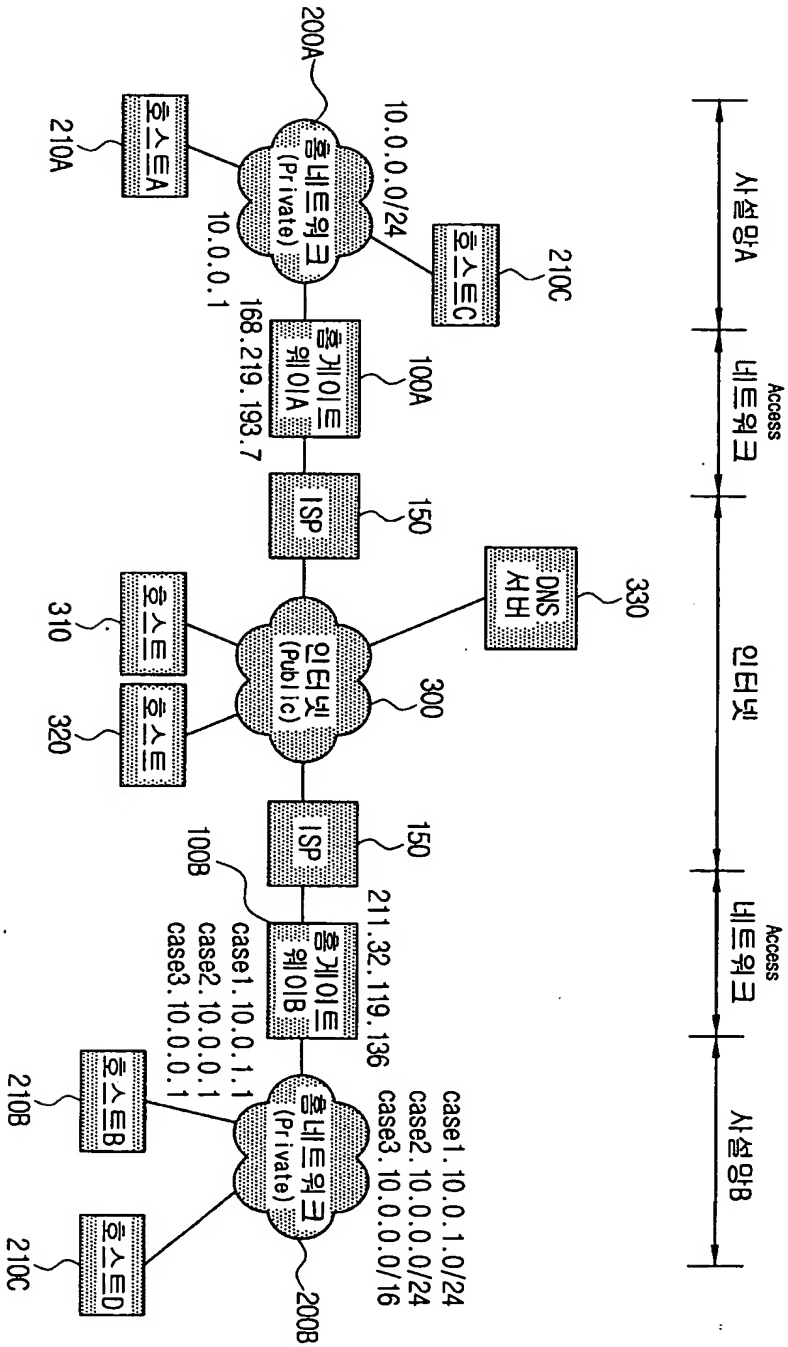
【청구항 6】

제 2항에 있어서,

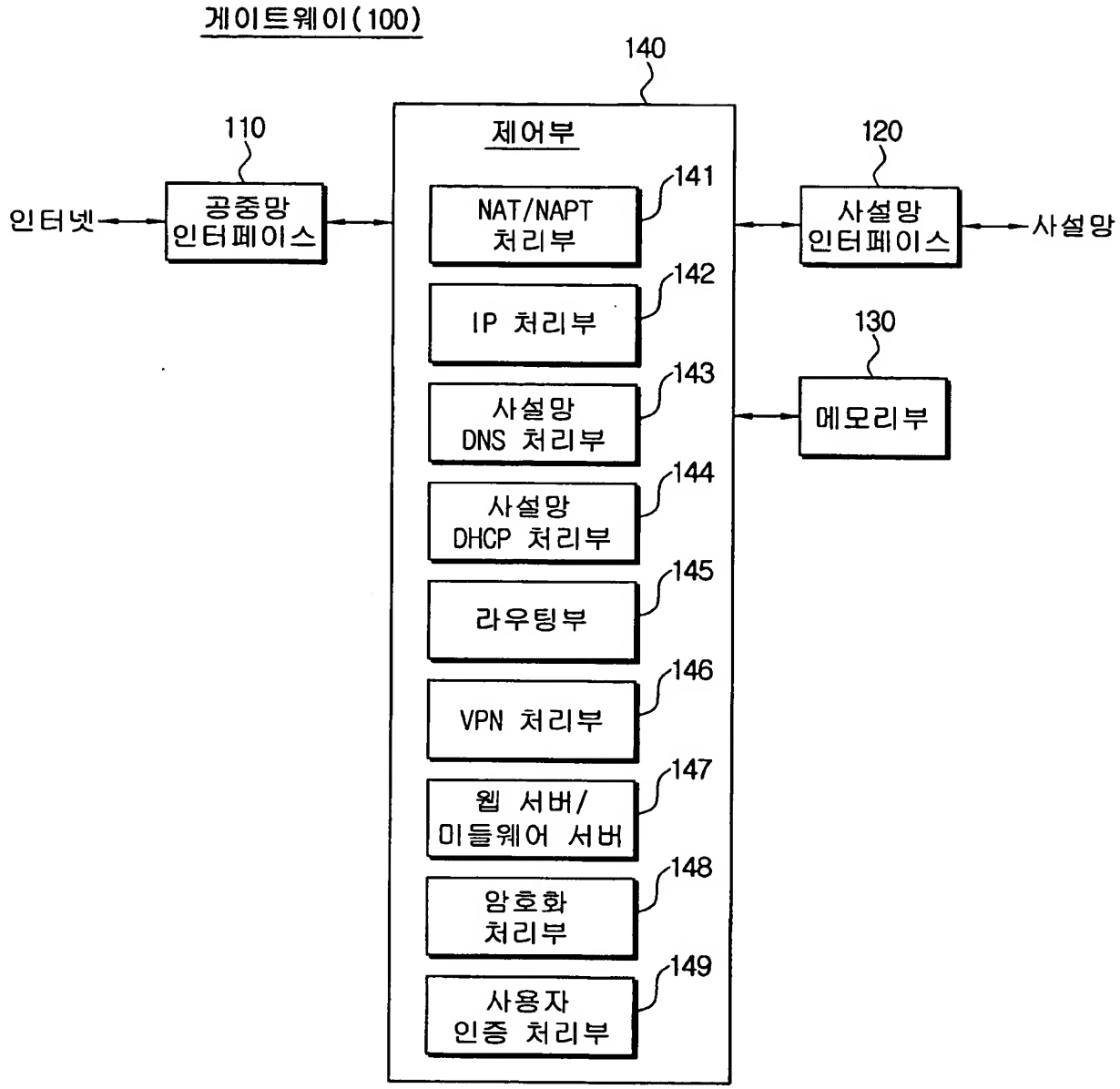
상기 웹서버는, 미들웨어서버로 대체 가능한 것을 특징으로 하는 망접속장치.

【도면】

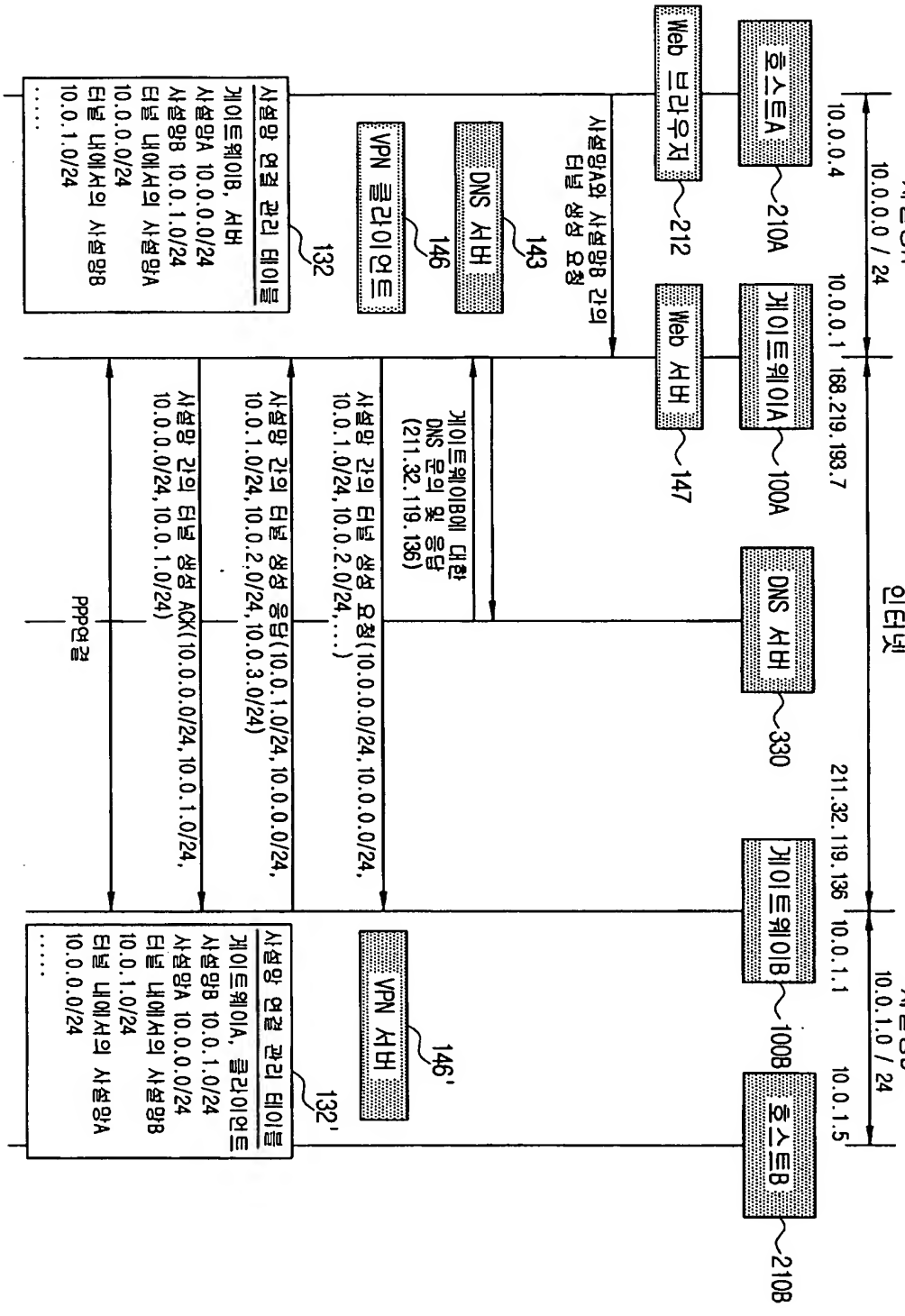
【도 1】


사설망A
Access 네트워크
인터넷
Access 네트워크
사설망B
200A
호스트A
210A
홈네트워크 (Private)
10.0.0.0/24
10.0.0.1
호스트C
210C
홈게이트웨이A
100A
168.219.193.7
ISP
150
DNS 서버
330
호스트
310
호스트
320
인터넷 (Public)
300
ISP
150
100B
211.32.119.136
홈게이트웨이B
case1.10.0.1.1
case2.10.0.0.1
case3.10.0.0.1
case1.10.0.1.0/24
case2.10.0.0.0/24
case3.10.0.0.0/16
호스트B
210B
홈네트워크 (Private)
200B
호스트D
210C

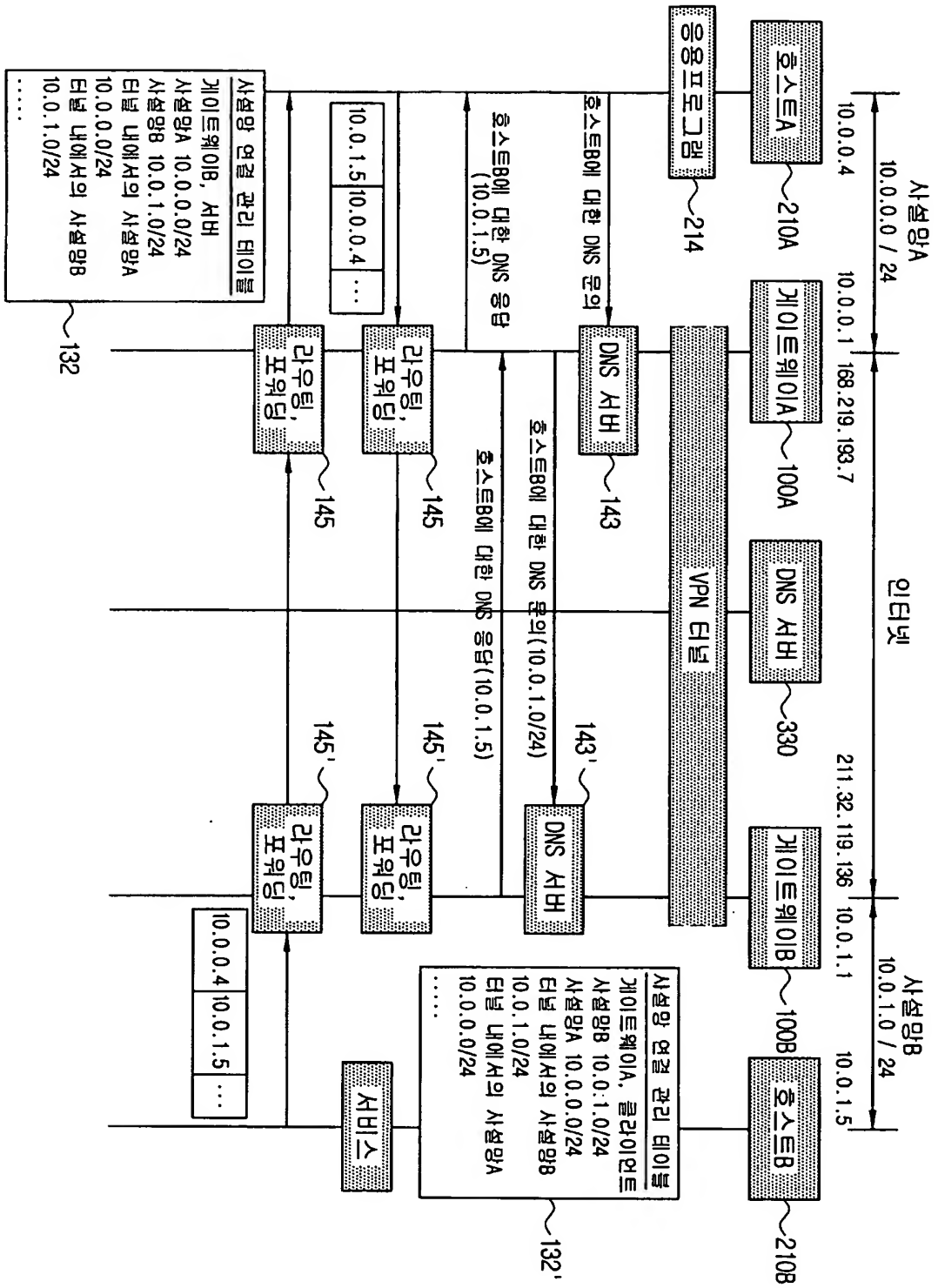
【도 2】


게이트웨이(100)
140
제어부
110
공중망 인터페이스
인터넷
141
NAT/NAPT 처리부
142
IP 처리부
143
사설망 DNS 처리부
144
사설망 DHCP 처리부
145
라우팅부
146
VPN 처리부
147
웹 서버/ 미들웨어 서버
148
암호화 처리부
149
사용자 인증 처리부
120
사설망 인터페이스
사설망
130
메모리부

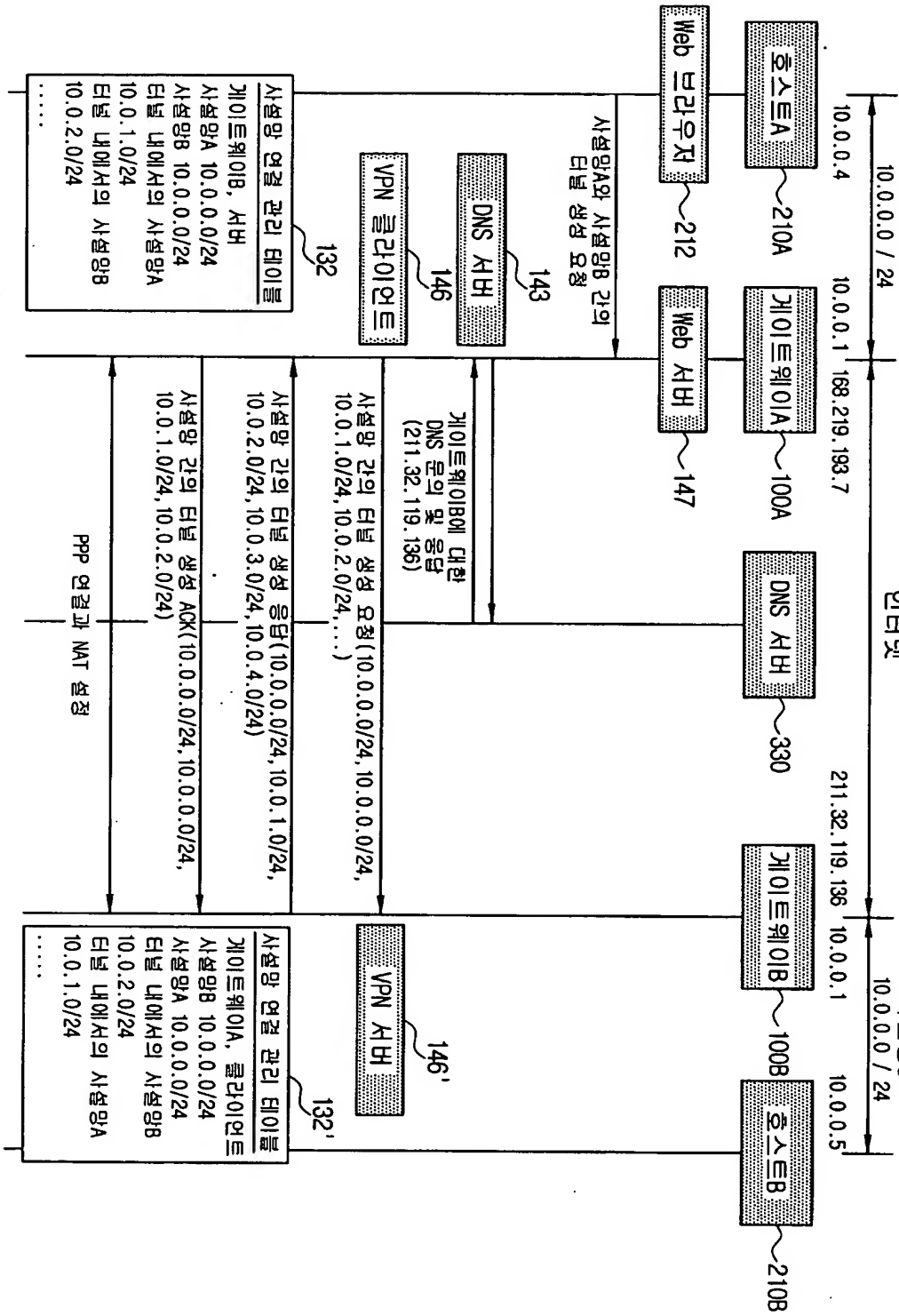
【도 3】


사설망A
10.0.0.0 / 24
10.0.0.4
10.0.0.1
호스트A
210A
게이트웨이A
100A
Web 브라우저
212
Web 서버
147
사설망A와 사설망B 간의
터널 생성 요청
DNS 서버
143
VPN 클라이언트
146
사설망 연결 관리 테이블
게이트웨이B, 서버
사설망A 10.0.0.0/24
사설망B 10.0.1.0/24
터널 내에서의 사설망A
10.0.0.0/24
터널 내에서의 사설망B
10.0.1.0/24
.....
132
168.219.193.7
인터넷
211.32.119.136
DNS 서버
330
게이트웨이B
100B
호스트B
210B
10.0.1.1
10.0.1.5
사설망B
10.0.1.0 / 24
게이트웨이B에 대한
DNS 문의 및 응답
(211.32.119.136)
사설망 간의 터널 생성 요청(10.0.0.0/24,10.0.0.0/24,
10.0.1.0/24,10.0.2.0/24,...)
사설망 간의 터널 생성 응답(10.0.1.0/24,10.0.0.0/24,
10.0.1.0/24,10.0.2.0/24,10.0.3.0/24)
사설망 간의 터널 생성 ACK(10.0.0.0/24,10.0.1.0/24,
10.0.0.0/24,10.0.1.0/24)
PPP연결
VPN 서버
146'
사설망 연결 관리 테이블
게이트웨이A, 클라이언트
사설망B 10.0.1.0/24
사설망A 10.0.0.0/24
터널 내에서의 사설망B
10.0.1.0/24
터널 내에서의 사설망A
10.0.0.0/24
.....
132'

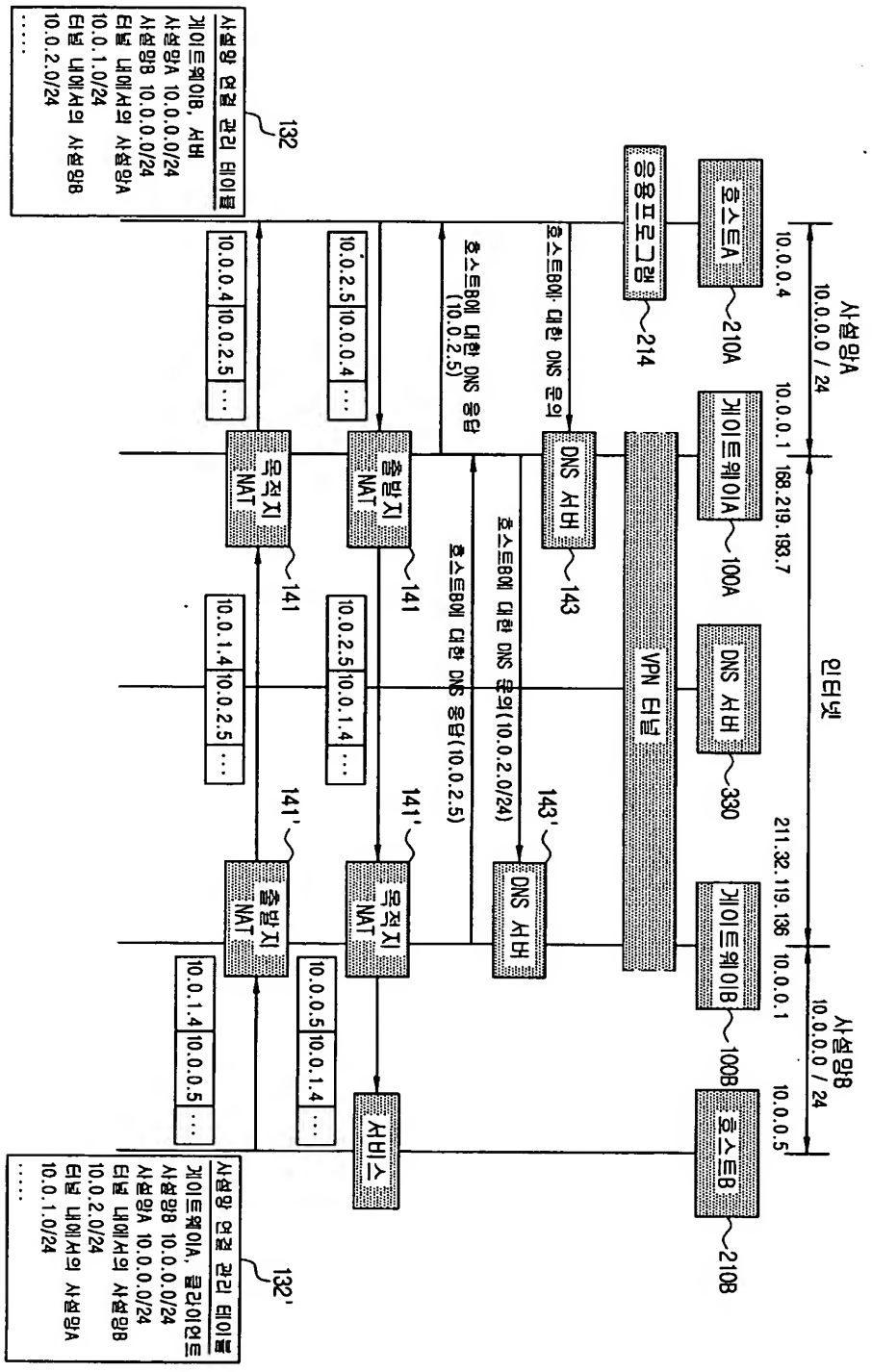
【도 4】


사설망A
10.0.0.0 / 24
10.0.0.4
10.0.0.1
호스트A
210A
게이트웨이A
100A
168.219.193.7
인터넷
211.32.119.136
10.0.1.1
게이트웨이B
100B
10.0.1.0 / 24
10.0.1.5
호스트B
210B
응용프로그램
214
VPN 터널
DNS 서버
330
호스트B에 대한 DNS 문의
DNS 서버
143
호스트B에 대한 DNS 응답
(10.0.1.5)
호스트B에 대한 DNS 문의(10.0.1.0/24)
143'
DNS 서버
호스트B에 대한 DNS 응답(10.0.1.5)
10.0.1.5
10.0.0.4
...
라우팅,
포워딩
145
145'
사설망 연결 관리 테이블
게이트웨이B, 서버
사설망A 10.0.0.0/24
사설망B 10.0.1.0/24
터널 내에서의 사설망A
10.0.0.0/24
터널 내에서의 사설망B
10.0.1.0/24
.....
132
사설망 연결 관리 테이블
게이트웨이A, 클라이언트
사설망B 10.0.1.0/24
사설망A 10.0.0.0/24
터널 내에서의 사설망B
10.0.1.0/24
터널 내에서의 사설망A
10.0.0.0/24
.....
132'
서비스

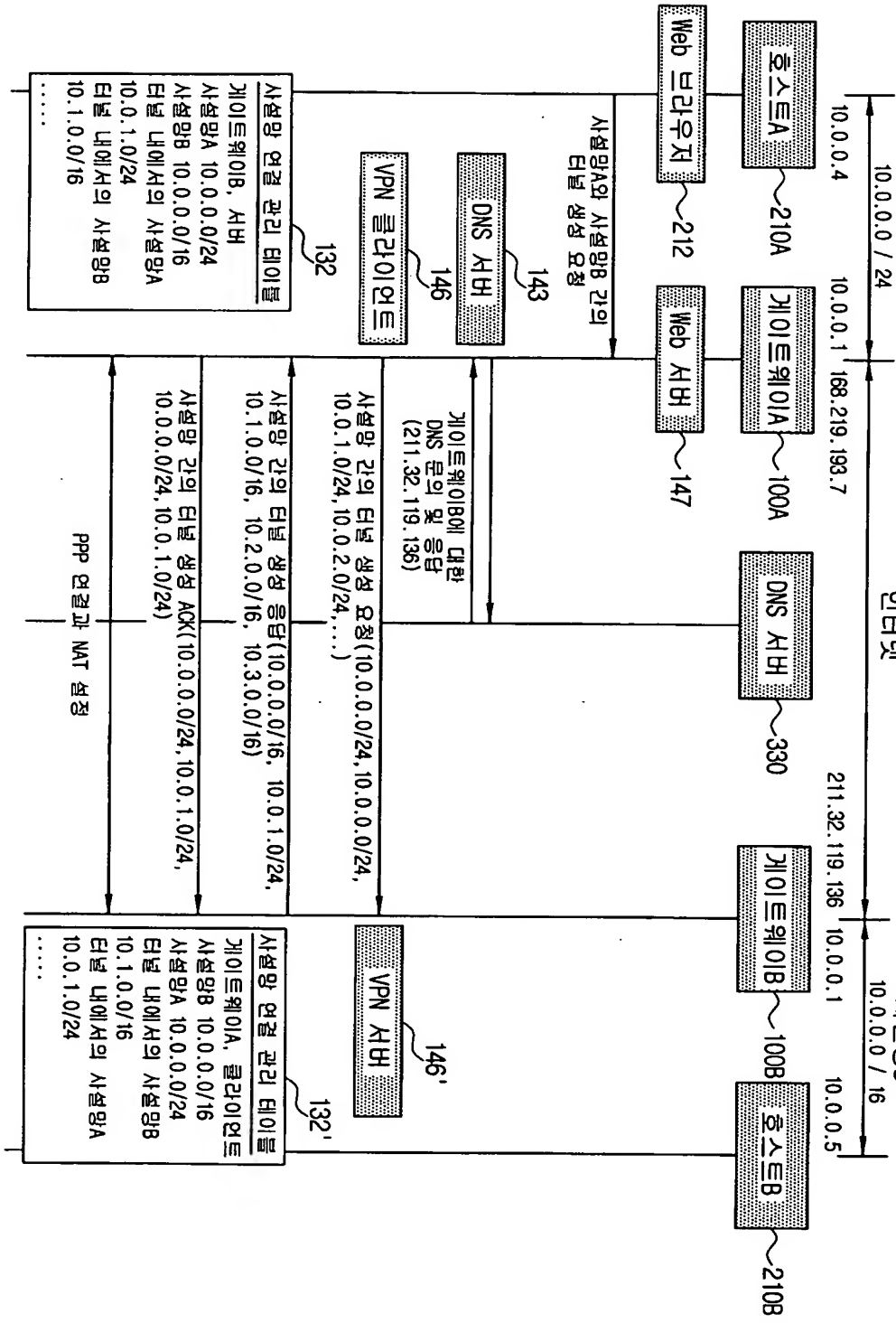
【도 5】


사설망A
10.0.0.0 / 24
10.0.0.4
10.0.0.1
호스트A
210A
게이트웨이A
100A
Web 브라우저
212
Web 서버
147
사설망A와 사설망B 간의
터널 생성 요청
DNS 서버
143
VPN 클라이언트
146
132
사설망 연결 관리 테이블
게이트웨이B, 서버
사설망A 10.0.0.0/24
사설망B 10.0.0.0/24
터널 내에서의 사설망A
10.0.1.0/24
터널 내에서의 사설망B
10.0.2.0/24
.....
인터넷
168.219.193.7
211.32.119.136
DNS 서버
330
게이트웨이B에 대한
DNS 문의 및 응답
(211.32.119.136)
사설망 간의 터널 생성 요청(10.0.0.0/24,10.0.0.0/24,
10.0.1.0/24,10.0.2.0/24,....)
사설망 간의 터널 생성 응답(10.0.0.0/24,10.0.1.0/24,
10.0.2.0/24,10.0.3.0/24,10.0.4.0/24)
사설망 간의 터널 생성 ACK(10.0.0.0/24,10.0.0.0/24,
10.0.1.0/24,10.0.2.0/24)
PPP 연결과 NAT 설정
사설망B
10.0.0.0 / 24
10.0.0.1
10.0.0.5
게이트웨이B
100B
호스트B
210B
VPN 서버
146'
132'
사설망 연결 관리 테이블
게이트웨이A, 클라이언트
사설망B 10.0.0.0/24
사설망A 10.0.0.0/24
터널 내에서의 사설망B
10.0.2.0/24
터널 내에서의 사설망A
10.0.1.0/24
.....

【도 6】


사설망A
10.0.0.0 / 24
10.0.0.4
호스트A
210A
10.0.0.1
게이트웨이A
100A
168.219.193.7
인터넷
211.32.119.136
게이트웨이B
100B
10.0.0.1
사설망B
10.0.0.0 / 24
10.0.0.5
호스트B
210B
응용프로그램
214
DNS 서버
143
VPN 터널
DNS 서버
330
DNS 서버
143'
서비스
호스트B에 대한 DNS 응답 (10.0.2.5)
호스트B에 대한 DNS 질의
호스트B에 대한 DNS 질의(10.0.2.0/24)
호스트B에 대한 DNS 응답(10.0.2.5)
목적지 NAT
141
출발지 NAT
141
출발지 NAT
141'
목적지 NAT
141'
132
사설망 연결 관리 테이블
게이트웨이B, 서버
사설망A 10.0.0.0/24
사설망B 10.0.0.0/24
터널 내에서의 사설망A
10.0.1.0/24
터널 내에서의 사설망B
10.0.2.0/24
.....
132'
사설망 연결 관리 테이블
게이트웨이A, 클라이언트
사설망B 10.0.0.0/24
사설망A 10.0.0.0/24
터널 내에서의 사설망B
10.0.2.0/24
터널 내에서의 사설망A
10.0.1.0/24
.....

【도 7】


사설망A
10.0.0.0 / 24
10.0.0.4
호스트A
210A
10.0.0.1
게이트웨이A
100A
168.219.193.7
인터넷
211.32.119.136
게이트웨이B
100B
10.0.0.1
사설망B
10.0.0.0 / 16
10.0.0.5
호스트B
210B
Web 브라우저
212
Web 서버
147
DNS 서버
330
VPN 서버
146'
사설망 연결 관리 테이블
게이트웨이A, 클라이언트
사설망B 10.0.0.0/16
사설망A 10.0.0.0/24
터널 내에서의 사설망B
10.1.0.0/16
터널 내에서의 사설망A
10.1.0.0/24
.....
132'
사설망A와 사설망B 간의
터널 생성 요청
DNS 서버
143
VPN 클라이언트
146
사설망 연결 관리 테이블
게이트웨이B, 서버
사설망A 10.0.0.0/24
사설망B 10.0.0.0/16
터널 내에서의 사설망A
10.0.1.0/24
터널 내에서의 사설망B
10.1.0.0/16
.....
132
게이트웨이B에 대한
DNS 문의 및 응답
(211.32.119.136)
사설망 간의 터널 생성 요청(10.0.0.0/24,10.0.0.0/24,
10.0.1.0/24,10.0.2.0/24,...)
사설망 간의 터널 생성 응답(10.0.0.0/16, 10.0.1.0/24,
10.1.0.0/16, 10.2.0.0/16, 10.3.0.0/16)
사설망 간의 터널 생성 ACK(10.0.0.0/24,10.0.1.0/24,
10.0.0.0/24,10.0.1.0/24)
PPP 연결과 NAT 설정